Security

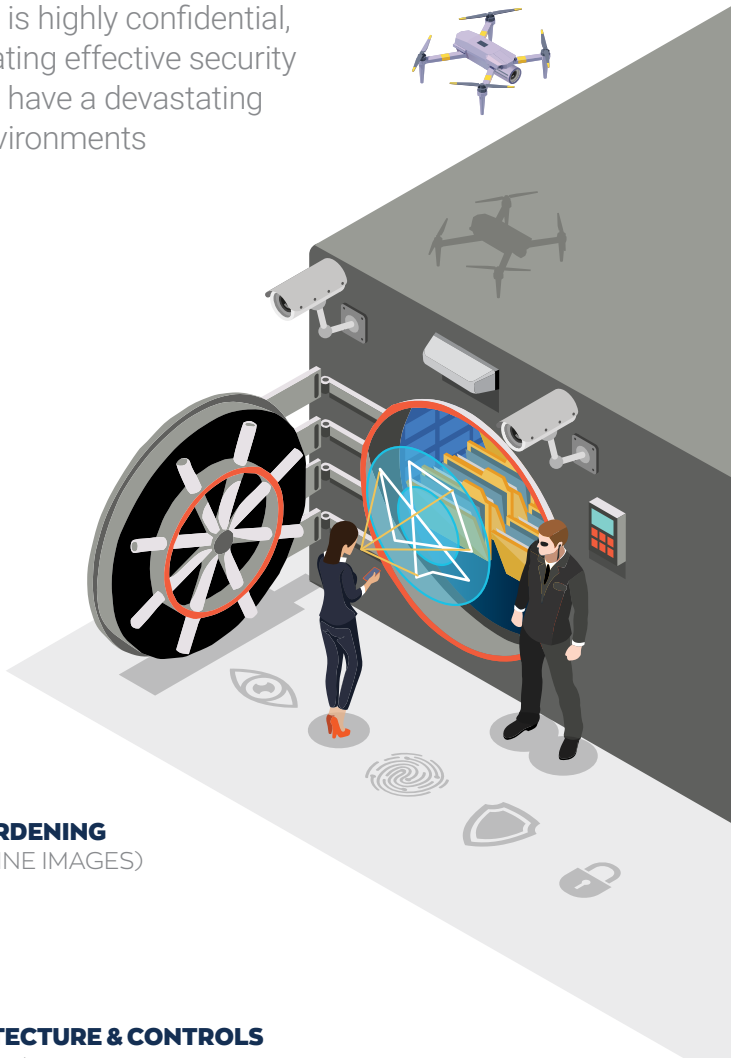
GEORGEJON

GEORGEJON.COM

Security as a Service

InfoSec without insomnia.

In industries across the business world, data platform security and protection is a costly and resource-intensive endeavor. In the eDiscovery realm, security and protection are mission-critical functions, as collected data is highly confidential, centralized, and a target for malefactors. Further complicating effective security management is that many security tools and controls can have a devastating impact on the performance and stability of eDiscovery environments due to the burst or surge amounts of data transmission, potentially resulting in dissatisfied clients and missed production deadlines.



Over the past 15 years, George Jon has worked hand in hand with our global pool of eDiscovery clients to balance security, performance, and cost initiatives relating to information security requirements and escalating/evolving user demands. After spending thousands of hours of researching, testing, implementing, and configuring security tools and controls, we have developed a holistic security management program that leverages state-of-the-art controls, industry-leading resources, and proven best practices to ensure the integrity and performance of client environments. And we can provide optimized outcomes at a fraction of cost of users trying to achieve success by themselves.

KEY TENETS OF SECURITY AS A SERVICE

IDENTITY & ACCESS MANAGEMENT

- Privileged access management (role-based access control)
- Password vaulting and rotation
- Multi-factor authentication
- Access audit and logging
- Single sign-on

VULNERABILITY MANAGEMENT

- Continuous vulnerability scanning across platform software systems
- Prioritized vulnerability patching, based on severity
- Ongoing vulnerability reporting and environment certificate monitoring

DATA ENCRYPTION

- Database Encryption – SQL TDE
- TLS 1.2 and SSL Certs for in-transit data
- Physical disk encryption for SAN natives
- vSphere encryption
- BYOK

APPLICATION HARDENING

(SECURITY BASELINE IMAGES)

- Relativity
- Nuix
- Brainspace
- Ipro

SECURITY ARCHITECTURE & CONTROLS

- Zone separation by tier
- Standardized, consistent use of IDS/IPS
- Traffic communication control
- Egress filtering and proxy internet access
- Change management, asset inventory tracking
- Data segregation

SIEM & SOC (OPTIONAL)

- Threat monitoring and alerting
- Threat hunting and pivoting
- Security log review
- Event correlation and retention